MATRIX Academic International Online Journal of Engineering and Technology
Volume VI Issue I, ISSN:2348-3326

Problems of improving transactions on the blockchain

D.T. Muhamediyeva [1] and A.N. Khudoyberdiev [2]

[1] "Tashkent Institute of Irrigation and Agricultural Mechanization Engineers" National Research University, Tashkent, Uzbekistan
[2] Research Institute for the Development of Digital Technologies and Artificial Intelligence, Tashkent, Uzbekistan
azizxudoyberdiyev707@gmail.com

Abstract. The article discusses the main directions of growth of the development of a decentralized system based on Blockchain technology. The system will make it possible to store all information on multiple computers, which will be available anytime, anywhere, without the participation of intermediaries. By employing Blockchain technology for the establishment of a global and distributed database, it is possible to ensure a completely transparent movement of electronic documents.

Keywords: Blockchain, Hash, Decentralized system, Transactions, Digital economy, Distributed ledger, Decentralization, Cryptocurrency.

1 Introduction

The digital economy operating on information technology platforms is developing rapidly, which requires the introduction of new models of such platforms. As the deployment of supercomputing capabilities and involvement with crypto-assets represent pivotal avenues for advancing the digital economy in numerous countries [1].

The public administration system needs to be strengthened, the investment climate for the introduction and growth of the digital economy needs to be improved, and conditions need to be established for the implementation of the "Strategy of Actions" on the five key areas of development for the Republic of Uzbekistan from 2017 to 2021 [2].

We live in the era of high technology. Technology has changed the way we work and see the world around us. It's been a considerable duration since smartphones were introduced, and observe how this innovation has influenced us! From placing orders to monitoring our account activities, we can efficiently handle all tasks using our mobile devices.

Presently, we find ourselves amidst another groundbreaking technology: blockchain technology. A blockchain network functions as a decentralized ledger capable of recording all transactions securely and efficiently between two parties. The main advantage of the blockchain network is decentralization and high transparency [3].

The notion of blockchain was first introduced in the year 1991 by research scientists Stuart Haber and W. Scott Stornett. Their main goal was to create a system of digital documents with a time stamp so that documents are not processed over time [4].

The system used a cryptographically secured block chain to store time-stamped documents, and in 1992 Merkle trees were introduced, making it more efficient by allowing multiple documents to be grouped into a single block. However, this technology was not used and the patent was revoked in 2004, four years before the creation of bitcoin [5].

At the end of 2008, a decentralized peer-to-peer electronic money system called “Bitcoin” was introduced, cryptography was sent by mail by an individual or group under the pseudonym Satoshi Nakamoto [6].

Proof of Work (PoW) is a decentralized peer-to-peer (P2P) protocol based on the Hashcash algorithm, but instead of using the reliable computing function of hardware like Reusable Proof of Work (RPoW), to protect bitcoins from double spending, and to track and verify transactions provided with in short, bitcoins are “mined” for rewards using a PoW mechanism for individual miners and then verified by decentralized nodes in the network [3].

Upon examination of blockchain technology, it becomes apparent that it has paved the path for various beneficial innovations. Bitcoin, a digital currency launched in 2009, stands as one such innovation within the realm of blockchain. In recent times, Bitcoin has experienced increasing success, boasting a capitalization ranging from 10 to 20 billion dollars. The use of currencies has been legalized in many countries, and bitcoins are being used for payments in many industries. Blockchain technology has been the foundation of bitcoins. In the present day, nearly every financial institution is investigating the potential benefits of blockchain technology and how it could be advantageous for their operations. Today, almost 15% of banks use the blockchain network [6].

With the development of blockchain technology, smart contracts appeared. Ethereum pioneered the use of smart contracts, which involve embedding computer programs directly into the blockchain network. This innovation enables the issuance of loans and bonds, distinguishing it from bitcoin cash tokens. Currently, the market value of the Ethereum smart-contract platform has reached billions [7].

Meanwhile, every computer on the network processes every transaction. This process is actually slow. A scalable blockchain network speeds up the process without compromising security. A scalable procedure essentially determines the required number of systems to validate each transaction and distributes the workload evenly. This method is anticipated to be exceptionally swift [5].

The mentioned information illustrates the challenging nature of the tasks undertaken by numerous cryptographers. Scientists and mathematicians have played a crucial role in the development of the blockchain network. Blockchain technology has simplified processes such as self-driving cars, drones, and international money transfers.

The future trajectory of blockchain technology remains uncertain for everyone. Technology continues to evolve. What we can hope for is that more and more people

adopt blockchain technology. Given how far blockchain has come, the future may come sooner than any of us imagine.

2 Opportunities In Blockchain

2.1 Transparency And Anonymity

Businesses are interested in blockchain technology primarily because it is virtually always open source. This implies that it can be altered as desired by other users or developers. The fact that open source makes it extremely impossible to change the recorded data on the blockchain is, however, what's most significant about it. Since the blockchain is a community of users, somebody will probably discover any changes to the data. Blockchain is hence a very secure technology.

2.2 Reduced Operating Costs

Blockchain enables transactions between individuals and businesses without the need of a middleman, frequently a bank. There won't be a need for brokers or stock exchanges to purchase and sell equities. The blockchain can actually cut expenses for the user or company over time since there is no need for any middleman or third party to act as an intermediary in transactions. When buying and selling anything directly from the buyer and seller, the fee that brokers charge can be significantly decreased. Brokers charge a percentage of the assets involved in a trade or transaction.

2.3 Faster Settlement of Transactions

Transactions often take a few days to settle in full for conventional banks and stock exchanges. The procedures set forth in banking and share transfer software, as well as the fact that financial institutions are only available during regular business hours, five days a week, are the major causes of this. Additionally, the fact that various financial institutions are spread out across several time zones might cause processing times to be delayed. Contrarily, because blockchain technology is operational around-the-clock, every day of the week, transactions based on it are completed much more quickly, if not instantaneously.

2.4 Decentralization

The absence of a central data center is a significant contributing factor to the effectiveness of blockchain technology. The blockchain empowers individual transactions with their distinct evidence of validity and authority, allowing for the enforcement of limits. This stands in contrast to traditional stock exchanges and institutions, which authenticate transactions through large centralized data centers. When data regarding a certain blockchain is divided into blocks and dispersed globally over different computers, it assures that, in the event that it falls into the wrong hands (such as those of a cybercriminal), only a tiny portion of the network may be compromised.

2.5 User Controlled Networks

The ability of blockchain to oversee transactions without the need for a centralized regulatory body has investors and consumers extremely enthusiastic. The users and developers are the ones who take ownership of the network, not a separate entity. Effective blockchain peer-to-peer connectivity can aid in the development of more efficient trading and transactional ecosystems. It will be simpler to operate and administer a sizable network of devices without any centralized controller by integrating it as a layer on top of the Internet.

2.6 Security

The lack of a central data center is a significant aspect contributing to the efficacy of blockchain technology. The blockchain allows individual transactions to possess unique evidence of validity and authority for enforcing limitations, unlike conventional stock exchanges and institutions that authenticate transactions through large centralized data centers. When data regarding a certain blockchain is divided into blocks and dispersed globally over different computers, it assures that, in the event that it falls into the wrong hands (such as those of a cybercriminal), only a tiny portion of the network may be compromised.

2.7 Methods

To hash the data obtained during the creation of Bitcoins, they use the SHA-256 encryption algorithm, which is also used in cryptography. It consists of encoding data of any size and type into a 256-bit key consisting of numbers and letters of the Latin alphabet.

The hash function is unique because it encodes both a multi-volume book and a single word, and the resulting hash value is the same size. If an attempt is made to modify at least 1 character of the original block, the resulting hash value will be radically different. This situation is called "avalanche effect" and serves to protect against changes. The SHA-256 algorithm guarantees protection against collisions, which means that the probability of creating random hashes with different input data tends to zero.

A blockchain is a linked list that contains data and a hash pointer to the block before it, forming a linked chain. Similar to a basic pointer, a hash pointer additionally stores a hash of the information from the preceding block in addition to the previous block's location. This minor adjustment is what makes blockchain so dependable. Consider for a moment that block 3 is attacked by hackers who attempt to alter the data. Due to the characteristics of hash functions, even a slight change in the data will significantly alter the hash. This implies that even little adjustments to block 3 will alter the hash.

The concept of hash trees was patented by Ralph Merkle in the year 1979(the patent expired in 2002).

A Merkle tree is a fully binary tree whose leaves contain the hashes of data blocks and whose inner leaves contain hashes consisting of the addition of values.

When considering a tree, you amalgamate every pair of leaves to generate a code. Merge two blocks to produce two hash pointers.

Subsequently, from the hash pointers produced by the left and right children, you form a hash pointer leading to the block containing the data. This process occurs recursively until reaching a hash header pointer that stores all the data. Bitcoin, Ethereum, Apache Cassandra, and various other systems employ Merkle trees (and variations) to offer:

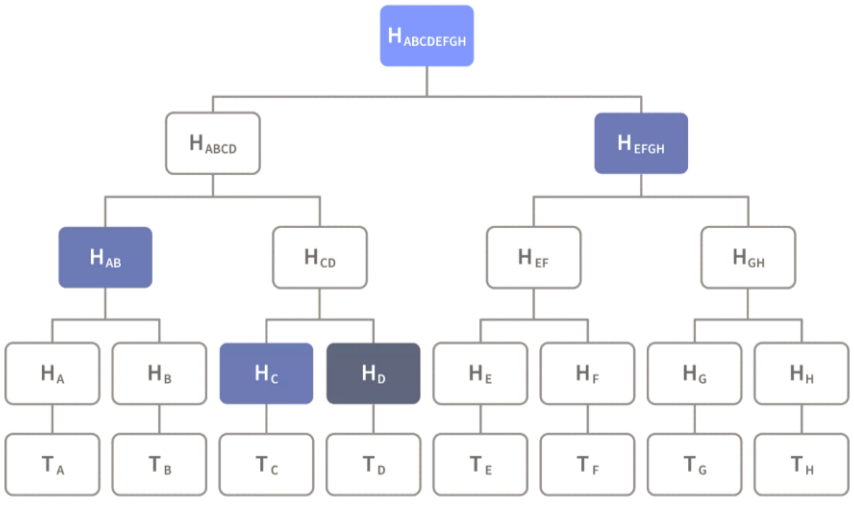
– compliance check;
– data verification;
– data synchronization.

Employing a hash tree, such as a Merkle tree:

– Substantially decreases the volume of data that a trusted entity must retain to validate the integrity of the data.
– Markedly diminishes network I/O required for ensuring data consistency, verification, and synchronization.
– Separates data verification from the data itself - A Merkle tree can live locally by a trusted authority or exist independently on distributed systems.

Data synchronization: Merkle trees prove valuable in harmonizing data across a distributed data store by enabling swift and efficient identification of altered records, eliminating the need for every node in a distributed system to compare all the data.

Instead, when a particular leaf in the tree is identified as altered, only the network linked to that specific leaf is transmitted through the network. It's important to note that Merkle trees lack mechanisms for conflict resolution and synchronization when multiple authors have the exact same record [5].



Picture 1. Merkle tree

Merkle trees provide an efficient solution for nodes in a network, saving both time and space. Constructing a Merkle tree from transaction data within each block enables the confirmation of transactions in logarithmic time rather than linear time.

Furthermore, this creates an opportunity for certain Bitcoin clients to conserve space by solely retaining the Merkle tree's root. There is no requirement to store every transaction that occurred in the entire history of Bitcoin, which is highly significant.

3 Results

The price market is not described as a market in which traders and stock brokers can buy and sell cheap paper, such as stocks and bonds, as well as other financial instruments. The conventional market capital system relies on centralized elements, encompassing the Stock Exchange, Settlement System, Clearing Chamber, and Centralized Depository as its primary components, shaping the traditional landscape of paper currency markets (see Fig. 1).

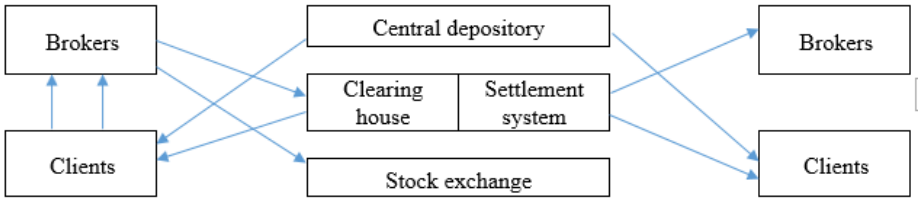


Fig. 1. Traditional stock market

The existing clearing and settlement procedure implemented by the Uzbek Stock Exchange is centralized, intricate, and requires T+2 days for transaction completion. A comparison between the current traditional system and the envisioned blockchain system is outlined in Table 1:

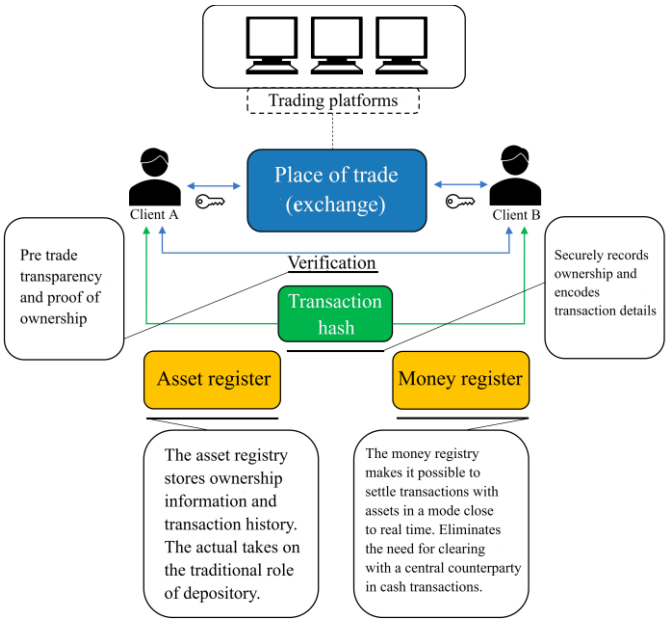
Table 1. Comparison between existing and proposed system

Parameters	Traditional	Proposed blockchain model
System	Centralized system	Decentralized system (identical data copies exist on all nodes)
Price	The expenses are elevated because of the involvement of intermediaries and brokers. Users are required to cover brokerage fees	Blockchain eliminates the need for third-party vendors or intermediaries, leading to reduced costs for users as they no longer have to pay brokerage fees

	and account maintenance charges	
Time	In the conventional system, settlement requires T+2 days. This prolonged timeframe is attributed to each institution maintaining its individual data copy, resulting in an extended approval process	The computation and reconciliation process will be expedited as a result of decentralization, given that identical data copies exist on all nodes
Immutability	Security systems installed but not fully protected from unauthorized (hacker) access	Blockchain ensures immutability, meaning that once transactions are recorded, they cannot be altered
Transparency	Low transparency	Enhanced transparency will prevent unjust trading practices, thereby fostering increased confidence in the market

Source: developed by the author based on bibliographic analysis

The inherent characteristics of blockchain, such as decentralization, distributed ledger, irreversibility, immutability, and real-time transactions, provide intrinsic advantages that the industry has been seeking for an extended period.
Now consider the structure of transactions when introducing blockchain technology to the stock market (see Fig. 2).



Source: developed by the author based on bibliographic analysis

Fig. 2. Making a transaction on the blockchain

Client A and client B meet at the trading venue and automatically verify that the other has the funds to complete the transaction (for example, client A clearly owns a security on the asset register and client B clearly owns the money on the cash register). Client A and Client B collaboratively authenticate the transaction by utilizing their respective private keys to unlock their assets or funds. Subsequently, they transfer ownership to the recipient through their keys. The authenticated transaction is then transmitted to the distributed ledger (blockchain) for verification and recording, with concurrent updates to the monetary ledger.

4 Summary

The digital economy encompasses more than just blockchain technology and its application in international financial markets or cryptocurrencies. While blockchain technology and cryptocurrencies are indeed components of the digital economy, the term specifically pertains to an economy driven by digital communications and information technology. In this context, it can also be seen as a mechanism for curbing the underground economy. This is attributed to the fact that all transactions will be electronically recorded, ensuring transparency. Moreover, the adoption of new IT technologies in production is expected to lead to a reduction in the cost of products and services.

The integration of blockchain and artificial intelligence holds the potential to unveil entirely novel opportunities and is presently concentrated on domains such as predictive models and investment platforms.

References

1. Son, PQ-4699, "Raqamli iqtisodiyot va elektron hukumatni keng joriy etish chora-tadbirlari to'g'risida," 28 April 2020.
2. Son, PF-4947, "O'zbekiston Respublikasini yanada rivojlantirish bo'yicha harakatlar strategiyasi to'g'risida," 07 February 2017.
3. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in 2017 IEEE International Congress on Big Data (Big Data Congress), Honolulu, 25-30 June 2017, pp. 557-564.
4. S. Haber and W. S. Stornetta, "How to time-stamp a digital document," J. Cryptology, vol. 3, pp. 99-111, 1991.
5. M. Iansiti and K. R. Lakhani, "The truth about blockchain," Harvard Business Review, Harvard University, January 2017.
6. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," bitcoin.org, October 2008.

7. G. Governatori, F. Idelberger, Z. Milosevic, R. Riveret, G. Sartor, and X. Xu, "On legal contracts, imperative and declarative smart contracts, and blockchain systems," Artificial Intelligence and Law, vol. 26, no. 4, p. 33, 2018.
8. T. Alam, "Blockchain and its role in the Internet of Things (IoT)," International Journal of Scientific Research in Computer Science, Engineering, and Information Technology, vol. 5, no. 1, 2019, doi: 10.32628/CSEIT195137.